Search and Seizure of Computers and Data
Outline of Presentations
July 8, 2004

I. Introductory Remarks

Hon. Jonathan Feldman, Western District of New York

II. Computer Search Methodology

Hon. Barbara Major, Southern District of California

- Search, Seize and Image
  - terms
  - seizure
  - imaging
    - logical v. physical copying
    - verification purposes
  - search or examination
  - on-site search v. on-site image and off-site examination v. seize, off-site image and examination

- On-site Search
  - generally impractical due to size of computers and other technical issues
  - creates proof problems if no image made b/c govt "entered" computer and changed data
  - preview to establish correct computer

- On-site Image and Off-site Examination
  - very common
    - legitimate businesses
    - where computer not instrumentality
  - permits owner to continue using computer and govt to have exact duplicate for evidentiary reasons
  - but problems may arise b/c environment is not controlled like a lab

- Seize Computer, Off-site Image and Examination
  - instrumentality of the crime
  - unusual computer configuration, hardware, software
  - return of property issues
    - Rule 41
    - return all non-authorized files/data
    - return image

- Warrant Return
  - computer equipment, image or documents
  - continue examining after return of warrant
  - additional return
  - plain view v. new warrant

2. Examination

- Issues to consider
  - forensic examination v. rummaging
  - degree of judicial oversight
  - privacy/irrelevant documents
  - potential difficulty in retrieving authorized documents
  - type, configuration and quantity of hardware/software
  - type of crime/investigation
  - evidence re hiding, deleting, or mislabeling
  - governmental resources

- Limitations
  - time
  - methodology
  - court updates

- Time Limits
  - time to image
  - time to examine
  - initially in warrant
  - potential extensions based on status reports
  - in motion to suppress evidence

- Methodology Limits
  - area of computer/hard drive or specific software applications
  - type of files
  - search terms (key words, dates etc)
  - automated v. manual searches

III. Fourth Amendment Considerations in the Search of Seizure of Computers and Data

Hon. Nan Nolan, Northern District of Illinois

1. Applying the Particularity Requirement to Computer Search Warrants

- Overview of the similarities and differences between a computer search and the search of a file cabinet

2. Applying the "Plain View" Doctrine to Computer Searches

3. Requiring A Description of the Computer Search Protocol in the Warrant Application

- *In the Matter of the Search of 3817 W. West End, First Floor*, --- F.Supp.2d ---, 2004 WL 1380272 (N.D. Ill. May 27, 2004).

- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, United States Department of Justice, Executive Office for United States Attorneys, Office of Legal Education at 100 (2d ed. 2002).

4. Cases Upholding "Sufficiently Specific" Computer Search Warrants

5. Court's Authority to Require a Search Protocol

- *In the Matter of the Search of 3817 W. West End, First Floor*, --- F.Supp.2d ---, 2004 WL 1380272 (N.D. Ill. May 27, 2004).

- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, United States Department of Justice, Executive Office for United States Attorneys, Office of Legal Education at 100 (2d ed. 2002).

IV. Available Search Technologies

Kenneth J. Withers, Senior Judicial Education Attorney, Federal Judicial Center

1. Identifying the computer

- Identifying computers
- Searching history files
- IP addresses

2. Securing the evidence

- Bitstream imaging
- Using appropriate forensic tools

3. Searching for "apparent" data

- Keyword searching
- Concept searching
- Searching for file attributes
- Searching for file types
- Hash value matching

4. Digging deeper

- Searching for deleted data
- Searching for residual data
- Searching for hidden drives

Search and Seizure of Computers and Data
Annotated Bibliography
June 25, 2004

Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997). Seizure of a computer pursuant to a warrant was not invalidated by the incidental, concomitant seizure of the computer s innocent contents, such as email messages and stored software, particularly where the computer was an instrumentality of the crime.

U.S. v. Bach, 310 F.3d 1063 (8th Cir. 2002), *cert. denied*, 538 U.S. 993 (2003). Internet Service Provider (ISP) technicians searched defendant s email account for child pornography pursuant to a warrant faxed to them by a government agent. The fact that no government agent was present during the search was not a Fourth Amendment violation because the expertise of the ISP technicians to conduct the search far outweighed that of the agents, the items seized were located on the ISP s property, the search was authorized by a judge, and government agents complied with all provisions of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701.

U.S. v. Bailey, 272 F. Supp. 2d 822 (D. Neb. 2003). Defendant s subscription to the candyman e-group, an internet site that frequently, obviously, unquestionably and sometimes automatically distributes child pornography to other subscribers established probable cause for a search of the subscriber's computer, even though there is no direct evidence that the subscriber actually received child pornography. *See also U.S. v. Shields*, 2004 WL 832937 (M.D. Pa. 2004) (denying defendant s motion to suppress evidence in factually similar case and concurring with *Bailey* s reasoning).

U.S. v. Barth, 26 F. Supp. 2d 929 (W.D. Tex. 1998). After repairman s inadvertent discovery of child pornography, agents conducted a broader, warrantless search of the computer in order to find additional evidence. The defendant s expectation of privacy in his computer files was not lost by turning the computer over for repairs, thus the agents computer search required a warrant to the extent that it exceeded the scope of the repairman s private search . The defendant s motion to suppress all evidence was granted.

U.S. v. Brunette, 76 F. Supp. 2d 30 (D. Me. 1999), *aff d*, 256 F.3d 14 (1st Cir. 2001). The District Court suppressed evidence gathered from defendant s computer after expiration of warrant s deadline for

completing the search. *But see U.S. v. Hernandez*, 183 F. Supp. 2d 468 (D. P.R. 2002) (evidence obtained by searching a seized computer five weeks after expiration of the search warrant was admissible). On strength of remaining, admissible evidence, defendant was convicted of possession of child pornography. On appeal, the court held that the original search warrant erroneously relied on officer s conclusory assertion that certain images met the statutory definition of child pornography. Absent independent review of the images by a judge or a more specific description of the images, the warrant lacked probable cause. Nevertheless, evidence seized under the warrant was admissible under the good faith exception to exclusionary rule. Defendant s conviction was affirmed.

U.S. v. Campos, 221 F.3d 1143 (10th Cir. 2000). Warrant authorizing seizure of all computer equipment which may be, or [is] used to depict child pornography was not overbroad since the warrant application explained why on-site search was infeasible, the computer equipment was a probable instrumentality of the crime, and the warrant limited the scope of subsequent off-site search to child pornography related files.

U.S. v. Carey, 172 F.3d 1268 (10th Cir. 1999). While conducting authorized search of defendant s computer for evidence of drug related crimes, agent discovered a file containing child pornography. Subsequent search for more child pornography evidence exceeded the scope of the warrant and was an unconstitutional general search. Neither the defendant s consent to a search of his apartment nor the plain view doctrine justified the agent s warrantless search for evidence of a non-drug related crime. The 10th Circuit reversed the lower court and granted defendant s motion to suppress. *But see U.S. v. Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999) (child pornography discovered while searching for evidence of computer hacking crimes was admissible under plain view); *U.S. v. Wong*, 334 F.3d 831 (9th Cir. 2003) (child pornography discovered while searching for evidence relating to murder of defendant s girlfriend was admissible under plain view).

U.S. v. Caron, 2004 WL 438685 (D. Me. 2004). Computer repairman inadvertently found between five and seven images of child pornography while repairing defendant s computer. An agent asked repairman to open one such file prior to obtaining a search warrant. Fourth Amendment was not violated because the agent did not exceed the scope of repairman s private search.

U.S. v. Cervini, 16 Fed. Appx. 865 (10th Cir. 2001). The fact that an ISP account registered to defendant and listing his home address was

used to post child pornography on the internet gave rise to probable cause to search the defendant s home and home computer.

U.S. v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997). Defendant did not have a reasonable expectation of privacy in child pornography related e-mails sent to an online chat room, thus messages collected from the chat room by government agents were admissible. Defendant s wife did not validly consent to search of the home when agents interrogated her and her teenage son at length and then threatened to execute their search warrant by breaking down the door to the home if she refused. Nevertheless, since the agents possessed a valid warrant at the time of the search, evidence was admissible under the inevitable discovery exception to the exclusionary rule.

U.S. v. Fantauzzi, 260 F. Supp. 2d 561 (E.D.N.Y. 2003). In charges stemming from defendant s membership in the child pornography related candyman e-group, defendant s motion to withdraw guilty plea was denied. Although the evidence against the defendant was obtained under the same affidavit found defective in *U.S. v. Perez*, 247 F. Supp. 2d 459 (S.D.N.Y. 2003), *Perez* did not control this case because motions to withdraw guilty pleas and motions to suppress are decided under different standards. *See also U.S. v. Schmidt*, 96 Fed. Appx. 41 (2d Cir. 2004); *U.S. v. Hudak*, 2003 WL 22170606 (S.D.N.Y. 2003).

U.S. v. Fiscus, 2003 WL 1963212 (10th Cir. 2003). After receiving a tip that defendant possessed child pornography in violation of his parole, agents conducted a warrantless search of defendant s home and seized a home computer and co-located diskettes. Neither the original home search nor agents subsequent warrantless search of the computer and seized diskettes violated the Fourth Amendment, because warrants are not required for parole searches. *See also U.S. v. Tucker*, 305 F.3d 1193 (10th Cir. 2002).

U.S. v. Gawrysiak, 972 F. Supp. 853, *aff d*, 178 F.3d 1281 (3d Cir. 1999). It was not unreasonable for agents to copy all of defendant s computer files without ascertaining which files fell within the scope of warrant when evidence indicated that defendant s business dealings were pervaded by fraudulent activity, selection and copying of only crime-related computer files was likely to be time consuming, and file copying was chosen over outright seizure of defendant s computer as least intrusive search method available.

U.S. v. Gleich, 293 F. Supp. 2d 1082 (D. N.D. 2003). Agents did not exceed the scope of a warrant authorizing the search of defendant s

home and home computer by seizing and searching three computers found in the home, since any of the three could have contained the evidence of child pornography that investigators were seeking.

U.S. v. Grant, 218 F.3d 72 (1st Cir. 2000), *cert. denied*, 531 U.S. 1025 (2000). Evidence showing that screen name registered to defendant was used to access child pornography while defendant was physically present in the home gave rise to probable cause to search defendant s home.

U.S. v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999). Agent s routine practice of opening virtually every single file contained in computer hard drive was not an unconstitutional general search. Defendant was exceptionally computer savvy and evidence of computer hacking could have been stored anywhere on the computer. Thus, child pornography related files discovered while agent was searching for hacking evidence were in plain view . *See also U.S. v. Wong*, 334 F.3d 831 (9th Cir. 2003) (child pornography discovered while searching for evidence relating to murder of defendant s girlfriend was admissible under plain view); *but see U.S. v. Carey*, 172 F.3d 1268 (10th Cir. 1999).

U.S. v. Greathouse, 297 F. Supp. 2d 1264 (D. Or. 2003). Agents obtained a search warrant for defendant s residence, a single-family home, which authorized the seizure of any and all computers and computer equipment that contained or depicted child pornography. Agents did not exceed the scope of the warrant by seizing all eight computers found in the residence, most of which did not belong to the defendant, because agents were unaware that the single-family home was shared by five adults. The court suggested in dicta that a more tailored search would likely have been required had agents known others resided in the home. Evidence was suppressed on other grounds, namely that the lapse of thirteen months between receipt of a tip that defendant possessed child pornography and warrant application rendered evidence too stale to support probable cause. *But see U.S. v. Lacy*, 119 F.3d 742 (9th Cir. 1997) (evidence was not stale despite lapse of ten months before warrant application); *U.S. v. Hay*, 231 F.3d 630 (9th Cir. 2000) (not stale despite six month lapse).

U.S. v. Grimes, 244 F.3d 375 (5th Cir. 2001). Fourth Amendment was not violated when agents viewed images discovered by a computer repairman because the agents did not exceed the scope of the repairman s private search. Defendant s possession of images of nude children constituted illegal possession of child pornography, although the children s private areas had been obscured using computer pixilation.

U.S. v. Habershaw, 2001 WL 1867803 (D. Mass. 2001). Agents arrived at defendant s residence to investigate reports of a man yelling obscenities at a group of small children. The defendant gave the agents permission to enter his apartment, where agents spotted a computer monitor displaying the message list of a child pornography related newsgroup. The defendant gave the agents permission to search the computer, and agents discovered child pornography. The court found that the defendant validly consented to the search; that the subsequent search warrant, authorizing the search of any and all computer equipment, was not overbroad; and that agents search of the computer after the warrant expired was not a second execution of the warrant or a failure to depart the premises as defendant claimed. The court denied the defendant s motion to suppress. *See also U.S. v. Hernandez*, 183 F. Supp. 2d 468 (D. P.R. 2002) (evidence obtained by searching a seized computer five weeks after expiration of the search warrant was admissible); *but see U.S. v. Brunette*, 76 F. Supp. 2d 30 (D. Me. 1999) (evidence suppressed when computer search conducted after warrant expired).

U.S. v. Hall, 142 F.3d 988 (7th Cir. 1998). Seizure of an entire computer was justified when the warrant narrowly described the child pornography files sought, since agents would not, under the terms of the warrant, be free to rummage through defendant s property.

U.S. v. Harding, 273 F. Supp. 2d 411 (S.D.N.Y. 2003). Warrant authorized agents to seize zip disks and to open and inspect their contents for evidence of fraud and possession of child pornography. Assuming that portion of warrant relating to child pornography lacked probable cause, child pornography evidence was nevertheless admissible under the inevitable discovery doctrine since agents would have discovered it while searching for fraud.

U.S. v. Hay, 231 F.3d 630 (9th Cir. 2000), *cert. denied*, 534 U.S. 858 (2001). Warrant authorizing generic seizure of all of defendant s hardware and software was sufficiently particular because government officials had no way of knowing where child pornography images might be stored. Lapse of six months between documented transmission of child pornography to defendant s computer and the government s application for a warrant did not render the application stale, since collectors of child pornography typically retain images for long periods of time. *But see U.S. v. Greathouse*, 297 F. Supp. 2d 1264 (D. Or. 2003) (lapse of thirteen months between government receiving tip that defendant possessed child pornography and warrant application rendered evidence too stale to support probable cause).

U.S. v. Hernandez, 183 F. Supp. 2d 468 (D. P.R. 2002). Noting that computer seizures are analogous to seizures of large quantities of paper documents, the court held that agents are permitted to remove computer equipment from searched premises and examine it at a later date without obtaining a warrant extension. Thus, in this case, evidence of child pornography uncovered during a computer search conducted five weeks after the original warrant expired was admissible. *See also U.S. v. Habershaw*, 2001 WL 1867803 (D. Mass. 2001) (agents search of seized computer after expiration of warrant was not second execution of the warrant or failure to depart the premises as defendant claimed, thus evidence was admissible); *but see U.S. v. Brunette*, 76 F. Supp. 2d 929 (W.D. Tex. 1998) (evidence suppressed when computer search conducted after warrant expired).

U.S. v. Hunter, 13 F. Supp. 2d 574 (D. Vt. 1998). During investigation of an attorney suspected of money laundering, a search warrant authorizing the seizure of all computers, storage devices, and software systems from the defendant violated the particularity requirement of the Fourth Amendment. However, the detailed search protocol attached to the warrant application assured that agents would retrieve relevant files without undue intrusion, thus the good faith exception to the exclusionary rule applied. When a computer search involves potentially privileged documents, screening should be performed by a special master or magistrate judge (although screening in this case by agents who were separated from prosecutor by a Chinese Wall was deemed acceptable).

U.S. v. Lacy, 119 F.3d 742 (9th Cir. 1997), *cert. denied*, 523 U.S. 1101 (1998). Lapse of ten months between transmission of images to defendant s computer and warrant application did not render evidence too stale to support probable cause since collectors of child pornography typically retain images for long periods of time. *But see U.S. v. Greathouse*, 297 F. Supp. 2d 1264 (D. Or. 2003). Generic seizure of computer equipment did not violate Fourth Amendment, since the warrant specified that only child pornography files would be searched. Under 18 U.S.C. § 2252(a)(4)(B), which requires that the defendant must knowingly possess 3 or more books, magazines, periodicals, films, video tapes, or other matter, matter describes the physical medium that contains the child pornography, not the image itself. Thus, the statute criminalizes possession of three or more computer storage devices containing child pornography, *not* three or more image files stored on those devices. Conviction affirmed. *But see U.S. v. Vig*, 167 F.3d 443 (8th Cir. 1999) (possession of three or more files stored on a single computer storage medium violates the statute).

U.S. v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996). Defendant had a reasonable expectation of privacy in his password-protected e-mails. A warrant authorized a search of *one* username associated with the defendant s America Online (AOL) e-mail account, but searches of *all* usernames billed to the defendant were conducted. Evidence gathered by searching the username account that was *not* listed in the warrant was suppressed. Defendant was originally convicted on four counts relating to using his computer to transport obscenity and child pornography; the appellate court vacated on two counts, affirmed on two counts, and remanded for a rehearing on sentence.

U.S. v. Perez, 247 F. Supp. 2d 459 (S.D.N.Y. 2003). Evidence that defendant subscribed to the child pornography related candyman e-group, absent affirmative evidence that defendant had actually downloaded, transmitted, or received child pornography, did not provide probable cause for search of defendant s home and seizure of his computer equipment. Defendant s motion to suppress granted. *See also U.S. v. Strauser*, 247 F. Supp. 2d 1135 (E.D. Mo. 2003) (same); *but see U.S. v. Bailey*, 272 F. Supp. 2d 822 (D. Neb. 2003) (concluding that the candyman investigation s defective affidavit did not necessitate suppression of evidence).

U.S. v. Rossby, 2003 WL 22682592 (9th Cir. 2003). Defendant s written consent to complete search of his office - including permission to seize any letters, papers, materials, or other property which [officers] may desire - reasonably included consent to search contents of defendant s laptop computers for evidence of mail and wire fraud.

U.S. v. Simons, 206 F.3d 392 (4th Cir. 2000), *cert. denied*, 534 U.S. 930 (2001). Where workplace had a clearly articulated policy of monitoring employee use of the internet, defendant, a government employee, did not have a reasonable expectation of privacy in files downloaded onto the hard drive of his office computer. Warrantless search of defendant s hard drive by remote computer and seizure of his hard drive without notice upon discovery that it contained child pornography did not violate the Fourth Amendment. *See also U.S. v. Bailey*, 272 F. Supp. 2d 822 (D. Neb. 2003) (defendant did not have a reasonable expectation of privacy in files on his workplace computer after agreeing to be monitored for appropriate use).

U.S. v. Slanina, 283 F.3d 670 (5th Cir. 2002), *vacated on other grounds*, 537 U.S. 802 (2002), *conviction aff d on remand*, 359 F.3d 356 (5th Cir. 2004). Defendant, a government employee, had a reasonable expectation of privacy in files stored on his work computer where employer did not inform employees that computer and internet

usage would be monitored. Nevertheless, after a computer repairman discovered evidence of child pornography on defendant s computer, government employer did not violate the Fourth Amendment by searching the computer as part of an investigation of work-related misconduct.

U.S. v. Smith, 27 F. Supp. 2d 1111 (C.D. Ill. 1998). Defendant s girlfriend, who contacted the police to report that child pornography was stored on defendant s home computer, validly consented to a warrantless search of the computer when the girlfriend lived in the defendant s home, had free physical access to the computer, the defendant had encouraged her and others to use the computer in the past, and the computer was not password protected.

U.S. v. Syphers, 296 F. Supp. 2d 50 (D. N.H. 2003). Government did not act unreasonably by detaining defendant s computer for seven months while searching for evidence of child pornography because investigators received a one year extension to the original warrant, they had an overwhelming backlog of computer crime investigations, and the search was necessarily time consuming because defendant possessed over 64,000 images of child pornography, some of which required de-encryption before they could be presented as evidence. *See also U.S. v. Greene*, 56 M.J. 817 (N.M. Ct. Crim. App. 2002) (retention of computer and disks for three months during investigation for possession of child pornography was reasonable when defendant consented to seizure, but "an excessively long period of retention, following a lawful seizure, could be unreasonable").

U.S. v. Tank, 200 F.3d 627 (9th Cir. 2000). Search of defendant s car incident to his lawful arrest, which resulted in the seizure of a ZIP disk later found to contain child pornography, was not a violation of the Fourth Amendment.

U.S. v. Triumph Capital Group, Inc., 211 F.R.D. 31 (D. Conn. 2002). In this public corruption case, a computer search warrant provided that agents would make every effort to review only those files that responded to a keyword search, since many documents contained on the computer were privileged. The warrant also approved agents use of a Chinese Wall taint-team procedure to screen out privileged documents. After conducting several key word searches, agents conducted a thorough, file by file search of the hard drive. Denying the defendants subsequent motion to suppress, the court held that keyword searches are of limited usefulness, thus agents acted reasonably by resorting to other search techniques. The fact that the warrant indicated a preference for a particular search methodology did not foreclose agents from using other methodologies.

U.S. v. Turner, 169 F.3d 84 (1st Cir. 1999). After obtaining defendant s consent to search his apartment in connection with an intruder s assault upon his next-door neighbor, an agent observed a photograph of a nude woman on defendant s computer. Agent searched the computer for more such images and discovered evidence of child pornography. The District Court granted defendant s motion to suppress, since the computer search exceeded the scope of defendant s original consent to search. The First Circuit affirmed.

U.S v. Upham, 168 F.3d 532 (1st Cir. 1999), *cert. denied*, 527 U.S. 1011 (1999). Warrant authorizing generic seizure of any and all computer software and hardware was not unconstitutionally overbroad when there was probable cause to believe that computer had been used to store and transmit images of child pornography. Prior to seizure the defendant had deleted some 1400 pornographic images which the government uncovered using a specialized utility program. This did not exceed the authority of the warrant, which was concerned with *what* could be searched, not with *how* the search was to be carried out.

U.S. v. Vig, 167 F.3d 443 (8th Cir. 1999). Possession of three or more images stored on *one* computer hard drive satisfies the requirement that the defendant must knowingly possess 3 or more books, magazines, periodicals, films, video tapes, or other matter depicting a minor in a sexually explicit manner. 18 U.S.C. § 2252(a)(4)(B). *But see U.S. v. Lacy*, 119 F.3d 742 (9th Cir. 1997).

U.S. v. Wong, 334 F.3d 831 (9th Cir. 2003). Child pornography discovered while searching defendant s computer for evidence related to girlfriend s murder was admissible under plain view doctrine. *See also U.S. v. Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999) (child pornography discovered while searching for evidence of computer hacking crimes was admissible under plain view); *but see U.S. v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (child pornography discovered while searching for evidence of drug-related crimes was not admissible under plain view).

U.S. v. Zimmerman, 277 F.3d 426 (3d Cir. 2002). An affidavit stating that defendant had been accused of sexually abusing minors and that he may have showed an image of adult pornography to minors six months prior did not provide probable cause for a search of defendant s home, including his home computer, for child pornography. The good faith exception to the exclusionary rule did not apply, since it was entirely unreasonable for agents to believe the warrant was valid. The District Court s order denying defendant s

motion to suppress was reversed, defendant s conviction and sentence were vacated, and the case was remanded.

Law Review Articles

Susan W. Brenner and Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 Mich. Telecomm. & Tech. L. Rev. 39 (2002), *available at* http://www.mttlr.org/voleight/Brenner.pdf.

Amy Baron-Evans, *When the Government Seizes and Searches Your Client s Computer*, 27 Champion Magazine 18 (June 2003).

Amy Baron-Evans and Martin F. Murphy, *The Fourth Amendment in the Digital Age: Some Basics on Computer Searches*, 47 B. B.J. 10 (June 2003).

Stephan K. Bayens, *The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?*, 48 Drake L. Rev. 239 (2000).

Hon. Robert H. Bohn, Jr. and Lynn S. Muster, *The Dawn of the Computer Age: How the Fourth Amendment Applies to Warrant Searches and Seizures of Electronically Stored Information*, 8 Suffolk J. Trial & App. Advoc. 63 (2003).

Jim Dowell, Note, *Criminal Procedure: Tenth Circuit Erroneously Allows Officers Intentions to Define Reasonable Searches: United States v. Carey*, 54 Okla. L. Rev. 665 (2001).

Rachel J. Hess, *Search and Seizure of E-Evidence in Illinois: Cybercrime and the Internet Frontier*, 91 Ill. B.J. 344 (2003).

Anton L. Janik, Jr., Article, *Combating the Illicit Internet: Decisions by the Tenth Circuit to Apply Harsher Sentences and Lessened Search Requirements to Child Pornographers Using Computers*, 79 Denv. U. L. Rev. 379 (2002).

Michael K. McChrystal, William C. Gleisner, III, and Michael J. Kuborn, *Law Enforcement in Cyberspace: Search and Seizure of Computer Data*, 71 Wis. Law. 35 (Dec. 1998).

Francisco J. Navarro, Comment, *United States v. Bach and the Fourth Amendment in Cyberspace*, 14 Alb. L.J. Sci. & Tech. 245 (2003).

Donald Resseguie, Note, *Computer Searches and Seizure*, 48 Clev. St. L. Rev. 185 (2000).

Carla Rhoden, *Challenging Searches and Seizures of Computers at Home or in the Office: From a Reasonable Expectation of Privacy to Fruits of the Poisonous Tree and Beyond*, 30 Am. J. Crim. L. 107 (2002).

Laurence H. Tribe, *The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier*, The Humanist, Sept.-Oct. 1991, at 15, *available at* http://www.sgrm.com/art1.htm.

Amy E. Wells, Comment, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 Okla. L. Rev. 99 (2000).

Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75 (1994).

Other Secondary Sources

Mitchell Kapor and Mike Godwin, *Civil Liberties Implications of Computer Searches and Seizures: Some Proposed Guidelines for Magistrates Who Issue Search Warrants*, *at* <http://www.sgrm.com/art-5.htm>

Robin Cheryl Miller, Annotation, *Validity of Search or Seizure of Computer, Computer Disk, or Computer Peripheral Equipment*, 84 A.L.R.5th 1 (2004).

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, United States Dept. of Justice, Sept. 2002, *at* <http://www.cybercrime.gov/s&smanual2002.htm>.

United States District Court,
N.D. Illinois,
Eastern Division.

In the Matter of the Search of: 3817 W. West End, First Floor Chicago, Illinois 60621

No. 04 M 108.
(2004 WL 1380272)

May 27, 2004.

MEMORANDUM OPINION AND ORDER

SCHENKIER, Magistrate J.

***1** On April 30, 2004, the Court issued a warrant that authorized the search of a home and the seizure of any computers that might be found, but that conditioned the search of the computer's contents upon the government providing the Court with a "search protocol" describing (a) the information the government sought to seize from the computer, and (b) the methods the government planned to use to locate that information without generally reviewing information on the computers that was unrelated to the alleged criminal activity. At the government's request, and so as not to jeopardize its ongoing investigation, the Court granted the government's motion to place the application and supporting affidavit under seal. On May 4, 2004, after the warrant had been executed and a computer and computer disks had been seized, the government orally requested that the Court allow the government to commence its search of the computer hard drive and disks without providing a protocol. The Court declined to do so.

Thereafter, on May 17, 2004, the government filed a written motion to reconsider, *ex parte* and under seal. In a meeting with the government on May 19, 2004, the Court orally denied the motion to reconsider, explaining the basis for its decision. The government requested that the Court make its ruling of record, which we do by this written opinion.

I.

We begin by recounting the relevant background events. Late in the afternoon of April 30, 2004, the government applied for the issuance of a search warrant for a residence at 3817 W. West End in Chicago, Illinois. The affidavit in support of the application set forth information offered by the government to establish probable cause to believe that Jacqueline Williams (also known by other names) was the occupant of that residence, and that she was engaged in acts of federal income tax fraud, in violation of 26 U.S.C. § 7206(2), in connection with her preparation and filing of federal income tax returns for various individuals during 2002 and 2003.

The government sought authority to search for and to seize certain enumerated items that it claimed would show the alleged tax fraud. However, with respect to any computers or related

media (generally referred to hereafter collectively as "computers"), the government sought a warrant authorizing it to seize those items before conducting any search of their contents for evidence of tax fraud (*see* Warrant, Attachment B, ¶ ¶ 5-8). The government explained that accountants and tax preparers who are engaged in tax fraud often use computers to prepare and retain records of fraudulent returns, that there was reason to believe that computers would be found at the 3817 W. West End residence, that the government would encounter significant obstacles in attempting to search the contents of any computers while at the residence, and that a search of the computers would be better conducted in a laboratory setting.

After reviewing the government's submission, the Court concluded that there was probable cause to believe that a search of Ms. Williams's residence at 3817 W. West End would yield evidence of the alleged federal income tax fraud. Accordingly, the Court informed the government that it would issue a warrant authorizing a search of the residence for items enumerated in Attachment B to the warrant, and the seizure of those items.

***2** However, the Court expressed concern over the request as it pertained to any computers the government might find at the residence. The Court was satisfied by the government's explanation of why a search of the contents of any computers while at the residence might not be practicable, and thus authorized the government to seize any computer without an on-site search of its contents. But, the Court explained to the government that a computer found during the search of a home likely would contain a wide variety of documents having nothing to do with the alleged criminal activity intermingled with documents that might fall within the scope of the alleged criminal activity. The affidavit provided no information that would suggest otherwise. Neither the application nor the affidavit set forth the types of documents relating to the alleged criminal activity that the government expected to find on the computers. Nor did the government's submission describe the means by which the government planned to search the computer, to avoid a general rummaging through all information on the computer, much of which would be irrelevant to the alleged criminal activity. To the contrary, the government represented that its search of the computer might involve *"an examin[ation of] all the stored data* to determine which particular files are evidence or instrumentalities of a crime" (Aff. in Support of Warrant Application, ¶ 36(a)) (emphasis added).

The Court told the government that in order to address these concerns, prior to allowing any search of the contents of the computers, the Court would require the government to provide a protocol outlining the methods it would use to ensure that its search was reasonably designed to focus on documents related to the alleged criminal activity. The purpose of this protocol was to provide the Court with assurance that the search of the computer after its seizure would not consist merely of a random or general examination of other documents--which, on a home computer, might contain sensitive information regarding health or other personal and private matters completely unrelated to the alleged criminal activity.

At that time, the government did not object to the requirement of a protocol, but asked whether the Court would require it to be provided before signing the warrant authorizing a search. In light of concerns expressed by the government that the search be conducted quickly because Ms. Williams might suspect that her activity had attracted the interest of the government, the Court decided to sign the warrant so that the search could proceed forthwith. However, the Court made

clear that if any computer was found, no search of its contents could commence before the government provided the required protocol. The Court made clear that the authority to seize the computers, and ultimately to search them, was conditioned on the government providing the required protocol.

The Court signed the search warrant at 5:40 p.m. on April 30. In order to prevent the ongoing investigation from being compromised, the Court granted the government's request that the application and affidavit submitted in support of the warrant be filed under seal. As reflected on the return of the warrant, the search began the next morning, May 1, 2004, at 7:30 a.m. The inventory attached to the return of the warrant shows that the government seized a number of items in connection with the search: including one computer (a Hewlett Packard Pavilion 700 computer) and an unspecified number of computer disks.

***3** On May 4, 2004, the government met with the Court to discuss the warrant. Attending the meeting were an attorney for the government (a different individual than the attorney who presented the warrant application on April 30), two agents, and an individual identified as the government's computer expert. The government attorney informed the Court that the search had been conducted, and that a computer had been seized. At that time, the government attorney argued that the government should be permitted to search the contents of the computer without providing the Court with any search protocol. The Court asked the government's computer expert about possible protocols, in order to determine whether there was some objection based on the view that a protocol was impracticable. While the Court considered it to be the responsibility of the government to offer the protocol it deemed best tailored to the search, the Court raised with the government possible ways of focusing the search of the computers, including: limiting the search to specific time periods; using key word searches; and/or limiting the search to text files and excluding graphics files. There was nothing in the responses by the government representatives that indicated that there was some technical or practical reason that a protocol could not be provided. [FN1]

> FN1. The Court notes that, in one respect, the response (or non- response) by the government was quite surprising. When the Court raised the possibility of limiting the search to certain time periods, one of the government representatives stated that such a limitation would not be helpful since the file directory only shows when a document was last saved. The Court then asked the government technical expert whether that problem could not be overcome by examining the "metadata" in the computer files, which would show not only the date a document was last saved, but also when the document was first created and (often times) the changes in the documents from the original draft to the final revision. *See* MANUAL FOR COMPLEX LITIGATION FOURTH at 78 (Federal Judicial Center 2004); *see also* THE SEDONA PRINCIPLES at 52 (The Sedona Conference 2004) ("Metadata is information about a particular data set which may describe, for example, how, when, and by whom it was received, created, accessed, and/or modified and how it is formatted. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept"). The government technical expert made no response, leaving the Court with the firm impression that he was not familiar with a

term that we would expect a computer expert to know.

What emerged clearly during the discussion was the government position that the Court lacked the authority to require a protocol. The government asserted that having found probable cause for a search, the Court's inquiry was at an end. In aid of that argument, the government analogized the search of a computer hard drive to the search of a file cabinet concerning papers: the government urged that just as the Court could not regulate the manner in which a file cabinet was searched, it could not regulate the conduct of the search of the computer files. The Court explained that it found this analogy unpersuasive, and that the Court believed it had the authority to require the search protocol. Accordingly, the Court reaffirmed that the government could not commence a search of the seized computer without first providing a search protocol.

Two weeks later, on May 17, 2004, the government filed a written motion, asking the Court to reconsider its requirement of a protocol. On May 19, 2004, the Court met informally with the government to discuss the motion. The Court explained that it had considered the government's arguments and authorities, but concluded that the Court possessed the power to require a search protocol, and that the power to do so was properly exercised here.

II.

The government's motion raises a serious question, one which we believe to be of first impression in this district: whether, when deciding to issue a warrant that would involve the seizure and subsequent search of a home computer, a magistrate judge has the authority to require the government to set forth a search protocol that attempts to ensure that the search will not exceed constitutional bounds. For the reasons set forth below, we believe that the answer to that question is yes.

A.

***4** A search warrant may issue only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. The Supreme Court has interpreted this provision to encompass three requirements: (1) that any warrants "must be issued by neutral, disinterested magistrates"; (2) that those seeking a warrant must show probable cause "to believe that 'the evidence sought will aid in a particular apprehension or conviction' for a particular offense"; and (3) that the warrants describe with particularity the " 'things to be seized,' as well as the place to be searched." *Dalia v. United States,* 441 U.S. 242, 255 (1979).

It is frequently said that the purpose of the particularity requirement is "to prevent a general exploratory rummaging in a person's belongings." *United States v. Carey,* 172 F.3d 1268, 1272 (10th Cir.1999) (citing *Marron v. United States,* 275 U.S. 192, 196 (1925)); *see also United States v. Stefonek,* 179 F.3d 1030, 1033 (7th Cir.1999) ("one of the purposes of the Fourth Amendment was to outlaw general warrants"). But, the particularity requirement serves another important purpose as well: it "assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to

search." *Groh v. Ramirez*, ___ U.S. ___, 124 S.Ct. 1284, 1292 (2004) (quoting *United States v. Chadwick*, 433 U.S. 1, 9 (1977)). When the warrant does not describe with particularity the things to be seized, it will not pass constitutional muster even if the application contains that information. *Groh*, ___ U.S. at ___, 124 S.Ct. at 1289 ("The fact that the *application* adequately described the 'things to be seized' does not save the *warrant* from its facial invalidity") (emphasis in original); *see also Stefonek*, 179 F.3d at 1033 ("The Fourth Amendment requires that the *warrant* particularly describe the things to be seized, not the papers presented to the judicial officer ...") (emphasis in original).

The degree of particularity that is required in any given situation may not be determined by resorting to some simple formulaic approach, but instead "varies depending on the circumstances of the case and the types of items involved." *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir.1986). A number of courts addressing the issue have found that the search and seizure of a computer requires careful scrutiny of the particularity requirement. *See United States v. Carey*, 172 F.3d 1268, 1275 n.7 (10th Cir.1999) ("the storage capacity of computers requires a special approach" in assessing the particularity requirement); *United States v. Barbuto*, No. 2:00CR197K, 2001 WL 670930, * 4 (D.Utah Apr. 12, 2001) ("searches on computers are unique because of their abundant storage capacity and the likelihood of discovering 'intermingled documents'..."); *United States v. Hunter*, 13 F.Supp.2d 574, 583-84 (D.Vt.1998) ("Computer searches present the same problem as document searches--the intermingling of relevant and irrelevant material--but to a heightened degree," which requires that each computer search be "independently evaluated for lack of particularity"). Likewise, we believe that a request for the search and seizure of computers merits a close look at the particularity requirement for several reasons.

***5** *First*, it is frequently the case with computers that the normal sequence of "search" and then selective "seizure" is turned on its head. Because of the difficulties of conducting an on-site search of computers, the government frequently seeks (and, as here, obtains), authority to seize computers without any prior review of their contents.

Second, that is significant in this case because of the substantial likelihood that the computer contains an "intermingling" of documents evidencing the alleged tax fraud, with documents that the government has no probable cause to seize. While the warrant application here established probable cause to believe that the computer may contain information of tax fraud, it did not contain information indicating that the computer contains nothing but information of tax fraud. The application contains no evidence that Ms. Williams's computer was dedicated solely to the alleged fraudulent activity; or that every return that Ms. Williams prepared was fraudulent; or that she did not use the computer for the full range of legitimate activities for which people typically use home computers. [FN2]

> FN2. The government's motion emphasizes that the Court orally stated during the May 4, 2004 meeting that there was "no question" that the application demonstrated probable cause for the search (Gov't Mot. to Reconsider, at 2). However, a showing of probable cause--no matter how strong--does not authorize a court to dispense with the independent requirement of particularity. *Groh*, ___ U.S. at ___, 124 S.Ct. at 1289 (a warrant that met

the probable cause requirement nonetheless was "plainly invalid" where it failed to satisfy the particularity requirement).

Third, we consider the extraordinary volume of information that may be stored even on a home computer. A megabyte of memory holds the equivalent of 500 typewritten pages of text. MANUAL FOR COMPLEX LITIGATION § 11.446, at 77. Even a modest home computer today frequently has 512 megabytes of memory (if not more), which translates into capacity of 256,000 pages of information. A floppy disk (some number of which were seized here) has a capacity of 1.44 megabytes, which translates into a capacity of 720 pages of plain text. *Id.* The capacity of the computer to store these large quantities of information increases the risk that many of the intermingled documents will have nothing to do with the alleged criminal activity that creates the probable cause for a search and seizure.

Fourth, while computers present the possibility of confronting far greater volumes of documents than are typically presented in a paper document search, computers also present the tools to refine searches in ways that cannot be done with hard copy files. When confronting a file cabinet full of papers, there may be no way to determine what to seize without doing some level of review of everything in the cabinet, as "few people keep documents of their criminal transactions in a folder marked '[crime] records." ' *Hunter,* 13 F.Supp.2d at 582 (quoting *United States v. Riley,* 906 F.2d 841, 845 (2d Cir.1990)). Thus, in that setting, it may be inevitable that innocuous records must be examined to determine whether they fall into the category of those papers covered by the search warrant. *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976).

By contrast, computer technology affords a variety of methods by which the government may tailor a search to target on the documents which evidence the alleged criminal activity. These methods include limiting the search by date range; doing key word searches; limiting the search to text files or graphics files; and focusing on certain software programs. *See Carey,* 172 F.3d at 1276. Of course, these are not the exclusive means of focusing a computer search, and they are not the means that might be appropriate in every case. But, the existence of these tools demonstrates the ability of the government to be more targeted in its review of computer information than it can be when reviewing hard copy documents in a file cabinet. [FN3]

FN3. In its oral presentation on May 4 (but not in its written motion), the government argued that a search protocol was not required by analogizing to the situation of the search of documents in a file cabinet. For the reasons stated above, we are persuaded that the analogy of the file cabinet to the computer is inadequate for purposes of the Fourth Amendment issue presented here, a conclusion that the *Carey* court also reached. *Carey,* 172 F.3d at 1275 ("Relying on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage" ') (citations omitted). Moreover, to the extent the government's analogy suggests that protocols are never used with respect to document searches, that suggestion is incorrect. In *Hunter,* the government's application for a search warrant included a protocol for the execution of the warrant that was designed to minimize the "invasion of materials protected by attorney-client privilege"--

whether in hard copy form or residing on a computer hard drive. *Hunter*, 13 F.Supp.2d at 578.

B.

***6** We now consider how these considerations relevant to computer searches affect the particularity requirement in this case. In so doing, we use the factors set forth in *Spilotro* in determining the degree of particularity required: "(1) whether probable cause exists to seize all items of a particular type described in the warrant, ...; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not, ...; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued." *Spilotro*, 800 F.2d at 963. We address each of these factors in turn.

First, there is probable cause to believe that there are some documents on the computers that constitute evidence of the alleged criminal activity. However, as explained above, those documents likely are intermingled with other, innocent materials in which the government has no interest. Thus, there is not probable cause to believe that everything on the computers is evidence of the alleged criminal activity.

Second, the warrant--as well as the application--fails to set forth "objective standards by which executing officers can differentiate items subject to seizure from those which are not." *Spilotro*, 800 F.2d at 963. The warrant merely describes the computers and related materials to be seized; it does not specify what objective standards the government proposes to use "to specify what types of files were sought in the searching of the two computers so that personal files would not be searched." *Barbuto*, 2001 WL 670930, *5; *see also* *Carey*, 172 F.3d at 1275 (when confronting a situation of intermingled computer documents, "law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in the warrant").

Third, we consider whether the government was able to provide a better description of how it seeks to go about searching the computer for information of criminal activity. " '[G]eneric classifications in a warrant are acceptable only when a more precise description is not possible." ' *United States v. Kow*, 58 F.3d 423, 427 (9th Cir.1995). The government has not even attempted to show that it cannot provide search criteria in the context of this warrant. [FN4]

FN4. The government makes a general argument that it would be "impractical" for the Court to "inquire as to how the government will conduct a search" (Gov't Mot. to Reconsider at 3 n.1). That argument fails to account for the tools that are available to create protocols to tailor computer searches, as other courts have recognized. The government's argument also fails to acknowledge that the Department of Justice has issued a manual stating that it often will be necessary to provide a search protocol in the context of a computer search: "The affidavit should also explain what techniques the agents expect to use to search the computer for specific files that represent evidence of

crime and may be intermingled with entirely innocuous documents." SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, United States Department of Justice, Executive Officer for United States Attorneys, Office of Legal Education at 100 (2d ed.2002) (hereinafter "DOJ MANUAL"). While the statements in the DOJ Manual do not represent the official position of the Department of Justice or other agencies, DOJ MANUAL at x, at a minimum the Manual further undermines the government's generalized assertion of "impracticality."

In addressing searches for hard copy documents and seizures of telephone communications, the Supreme Court has admonished that "responsible officials, *including judicial officers,* must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusion upon privacy. *Andresen*, 427 U.S. at 482 n.11 (emphasis added). That admonition applies with even more force in the context of computer searches, where the volume of intermingled documents may be substantial and there are tools to focus those searches that are unavailable for searches of hard copy documents. We conclude that, as a practical matter, the government can provide the Court with a protocol that would supply particularity to the search of the computers. And, we conclude that as a matter of constitutional law, the government must do so in order to satisfy the particularity requirement of the Fourth Amendment.

C.

***7** The government's core objection to providing a search protocol is that the Court is powerless to require it. That objection is inconsistent with the foregoing case law, *see, e.g., Carey* and *Barbuto,* as well as with the DOJ Manual, which notes that "[t]he reasons for articulating the search strategy in the affidavit are both practical and legal." DOJ MANUAL, at 101. Indeed, the government's notion that a judge is powerless to regulate the means of executing a search and seizure is belied by the government's own request in this case that the Court approve one particular method of executing the search: that is, to allow the government to seize the computers so that they may be searched off-site. That request, which is consistent with the position set forth in the DOJ Manual, *see* DOJ MANUAL at 100, 103, recognizes that practical considerations are relevant to delineating the means of a search. That is also the teaching of *Spilotro,* which looks to practical considerations in determining the degree of particularity required in a warrant.

We have considered the government's arguments that the Court lacks the authority to require a search protocol to give particularity to the search and seizure of the computers' contents. We find those arguments unpersuasive.

The government cites several "knock and enter" cases to argue that the Court has no authority to inquire in advance into the methods by which a warrant will be executed. *United States v. Banks*, ___ U.S. ___, 124 S.Ct. 521 (2003); *United States v. Basham*, 268 F.3d 1199 (10th Cir.2001). We view these cases as recognizing the reality that neither the government nor a judge can know in advance what situation may confront agents who approach a location to execute a search, and that, as a result, no one can say in advance how many knocks must be made on the door or how long a knock must go unanswered before entry. By contrast, when the government wishes to

search a computer hard drive in the controlled environment of a laboratory, it is not confronted with a rapidly evolving and sometimes dangerous situation that must be addressed on the spot.

Nor are we persuaded by the government's citation to *Dalia,* 441 U.S. at 257-58, in which the Supreme Court held that a warrant authorizing the installation of a wire intercept device was not defective because it failed to specify how the device would be installed. Indeed, while that case did not present the question of a judge's authority to specify the method by which government agents would listen in on intercepted calls; the Supreme Court noted with approval that the court issuing the warrant in fact had ordered the government "to take all reasonable precautions 'to minimize the interception of communications not otherwise subject to interception,' and required the officials to make periodic progress reports." *Dalia,* 441 U.S. at 242.

Finally, the government argues that having found probable cause and allowing the computers to be seized, the Court can do nothing more (Gov't Mot. to Reconsider, at 6, 8). At the threshold, this argument fails to acknowledge what the government elsewhere in its motion acknowledges (*id.* at 2): that the Court issued the warrant conditioned upon the government providing the protocol before there was a search of any computers. The Court imposed that requirement as a condition of signing the warrant because without a protocol, the warrant lacked particularity that would justify a search of the computers.

***8** Moreover, the government's argument erroneously conflates the probable cause and particularity requirements. As *Groh* recently reaffirmed in finding invalid a warrant that was based on probable cause but lacked particularity, these are independent requirements which must both be met. Here, while there was (and is) probable cause to believe that the computer contains some information that would constitute evidence of criminal activity, the warrant does not indicate what types of such information the government wishes to search for on the computer or how the government seeks to search for it in a way that will, to adapt the language of the *Dalia* court to the computer context, "minimize the [review] of [information] not otherwise subject to [review]." 441 U.S. at 242. In short, the Court imposed the requirement of a protocol to ensure that there was both probable cause and particularity before the government searched the computers.

D.

The government urges that any questions about the manner in which a search is executed may be addressed by a judge when approving the warrant, but only when a judge later is confronted with a motion to suppress. If adopted, such an approach would unnecessarily run the risk of the unfortunate results reached in *Carey* and *Barbuto,* where evidence seized in a search of a computer was suppressed because of a failure to provide the magistrate judge with search protocols. *Carey,* 172 F.3d at 1275 (in the case of intermingled documents, the magistrate judge should "require officers to specify in a warrant which type of files are sought"); *Barbuto,* 2001 WL 670930, *5 (methods or criteria by which a search of computer files would be conducted "should have been presented to the magistrate before the issuance of the warrants or to support the issuance of a second, more specific warrant once intermingled documents were discovered").

An approach that leads to such results is neither desirable nor legally required. We do not

believe that is the approach that the Supreme Court had in mind when it stated that "responsible officials, including judicial officials," must take care to assure that searches are conducted so as to "minimize [ ] unwarranted intrusions upon privacy." *Andresen*, 427 U.S. at 482 n.11. The purpose of review of warrant applications by "neutral, disinterested magistrates" is to ensure that the requirements of probable cause and particularity are met. When there are concerns about the particularity of a given search, as is the case here, it is both sensible and constitutionally required to address those concerns at the front end of the process, and to resolve them in a way that avoids the later suppression of evidence.

CONCLUSION

We emphasize that, in requiring a protocol here, the Court does not seek to dictate the specific criteria that the government may employ in order to supply particularity to its search and seizure of contents of the computers. Nor does the Court envision that a set of criteria initially approved will be forever set in stone; we do not foreclose the possibility that those criteria may need to be adjusted in response to what is found once the computer search commences. But, as matters now stand, what the government seeks is a license to roam through everything in the computer without limitation and without standards. Such a request fails to satisfy the particularity requirement of the Fourth Amendment, and the Court therefore will not approve it.

***9** Accordingly, the Court denies the government's motion to reconsider. In light of this ruling, the Court orders that within 21 days the government inform the Court in writing of the following: (a) whether there is good cause that this Opinion, which does not disclose sensitive material from the application, should remain under seal; and (b) whether the government still wishes to search the computer. If so, within that 21 day period the government shall submit for review a proposed protocol for searching the contents of the computer. If the government informs the Court that it no longer wishes to search the computer, then the Court will direct that the computer be returned.

UNITED STATES OF AMERICA, Plaintiff, v. JUSTIN BARRETT HILL, Defendant.

No. CR 02-01289 AK

UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA

2004 U.S. Dist. LEXIS 11116 (EXCERPTED)

June 17, 2004, Decided

DISPOSITION: [*1] Defendant's motion to suppress DENIED. Defendant's motion for discovery GRANTED.

COUNSEL: Teresa Mack, Assistant United States Attorney, Los Angeles, California, argued for the government.

Carlton F. Gunn, Deputy Federal Public Defender, Los Angeles, California, argued for defendant.

JUDGES: Alex Kozinski, United States Circuit Judge.

OPINIONBY: Alex Kozinski

OPINION: KOZINSKI, Circuit Judge. *

* Sitting by designation pursuant to *28 U.S.C. § 291(b)*.

[. . .]

2. Defendant argues that the warrant was overbroad because (a) it allowed seizure of all computer media without requiring inspection at the scene, even though the affidavit did not explain why such an inspection would not be feasible; and (b) it placed no limits or controls on the search methodology police used to analyze the seized media.

a. Search warrants must be specific. "Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *United States v. Towne, 997 F.2d 537, 544 (9th Cir. 1993)* (internal quotation marks and citations omitted). A warrant describing a category of items is not invalid if a more specific description is impossible. *United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986)*.

The level of specificity required "varies depending on the circumstances of the case and the type of items involved." *Id.*

The warrant here commanded [*16] the officers to search for and seize: "1) An IBM 'clone' medium tower personal computer ... 3) All storage media belonging to either item # 1 or the individual identifying himself as [defendant] at the location. 4) All sexually explicit images depicting minors contained in item # 3." Defendant argues the warrant was overbroad because it authorized seizure of storage media whether or not they contained child pornography. He suggests it should have authorized seizure only of media containing child pornography. But it is impossible to tell what a computer storage medium contains just by looking at it. Rather, one has to examine it electronically, using a computer that is running the appropriate operating system, hardware and software. The police had no assurance they would find such a computer at the scene--nor did they, for that matter--or that, if they found one, they could bypass any security measures and operate it.

Defendant suggests that the police could have brought their own laptop computer: Having probable cause to seize only computer storage media that contained certain types of files, the police should have been required to bring with them the equipment necessary to separate [*17] the sheep from the goats. Defendant's argument raises an important question about how police must execute seizures pursuant to a warrant. Because seizable materials are seldom found neatly separated from their non-seizable counterparts, how much separating must police do at the scene to avoid taking items that are neither contraband nor evidence of criminal activity?

As always under the *Fourth Amendment*, the standard is reasonableness. To take an extreme example, if police have probable cause to seize business records, the warrant could not authorize seizure of every piece of paper on the premises on the theory that the police conducting the search might not know how to read. The matter becomes more difficult if the police have cause to believe the records are not in English. Are the police required to bring with them at least one officer who can read the language of the documents and separate those that provide evidence of criminal activity from those that don't? The answer might turn on how readily the police can find an officer who is fluent in that language. In Los Angeles today, finding an officer who reads Spanish may be fairly easy, while finding one who can read Portuguese [*18] or Russian probably is not. Police are certainly not required to hire an expert translator to bring with them; they are entitled to limit the search team to officers already employed and reasonably available at the time the search is to be conducted. n10

> n10 Police are free to hire such experts to help them conduct a search, see, e.g., *Forro Precision, Inc. v. IBM, 673 F.2d 1045, 1053-54 (9th Cir. 1982)*, and it may well be praiseworthy for them to do so. See, e.g., *United States v. Tamura, 694 F.2d 591, 596 n.4 (9th Cir. 1982)*; see also *United States v. Wuagneux, 683 F.2d 1343, 1353 (11th Cir. 1982)* (lauding similar procedure as a way to "assure that [the search is] conducted in a manner that minimizes unwarranted intrusions into privacy." (internal quotation marks omitted)). But the *Fourth Amendment* does not require it.

Returning to defendant's case, the court concludes that the police were not required to bring with them equipment capable of reading computer [*19] storage media and an officer competent to operate it. Doing so would have posed significant technical problems and made the search

more intrusive. To ensure that they could access any electronic storage medium they might find at the scene, police would have needed far more than an ordinary laptop computer. Because computers in common use run a variety of operating systems--various versions or flavors of Windows, Mac OS and Linux, to name only the most common--police would have had to bring with them a computer (or computers) equipped to read not only all of the major media types, but also files encoded by all major operating systems. Because operating systems, media types, file systems and file types are continually evolving, police departments would frequently have to modify their computers to keep them up-to-date. This would not be an insuperable obstacle for larger police departments and federal law enforcement agencies, but it would pose a significant burden on smaller agencies.

Even if the police were to bring with them a properly equipped computer, and someone competent to operate it, using it would pose two significant problems. First, there is a serious risk that the police [*20] might damage the storage medium or compromise the integrity of the evidence by attempting to access the data at the scene. As everyone who has accidentally erased a computer file knows, it is fairly easy to make mistakes when operating computer equipment, especially equipment one is not intimately familiar with. The risk that the officer trying to read the suspect's storage medium on the police laptop will make a wrong move and erase what is on the disk is not trivial. Even if the officer executes his task flawlessly, there might be a power failure or equipment malfunction that could affect the contents of the medium being searched. For that reason, experts will make a back-up copy of the medium before they start manipulating its contents. Various other technical problems might arise; without the necessary tools and expertise to deal with them, any effort to read computer files at the scene is fraught with difficulty and risk.

Second, the process of searching the files at the scene can take a long time. To be certain that the medium in question does not contain any seizable material, the officers would have to examine every one of what may be thousands of files on a disk--a process [*21] that could take many hours and perhaps days. See pages 23-24 infra. Taking that much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive. Police would have to be present on the suspect's premises while the search was in progress, and this would necessarily interfere with the suspect's access to his home or business. If the search took hours or days, the intrusion would continue for that entire period, compromising the *Fourth Amendment* value of making police searches as brief and non-intrusive as possible.

Because of these considerations, the court concludes that the police were not required to examine defendant's electronic storage media at the scene to determine which contained child pornography and which did not. They were entitled to seize all such media and take them to the police station for examination by an expert. Accord *United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000)* (upholding, in a child pornography case, a warrant authorizing seizure of a defendant's entire computer system because the circumstances "justified taking the entire [computer] [*22] system off site because of the time, expertise, and controlled environment required for a proper analysis"); *United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999)* (holding, also in a case involving child pornography, that a warrant authorizing search and seizure of defendant's computer and all disks "was about the narrowest definable search and seizure reasonably likely to obtain the images" and that "a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or

drugs"); see also *United States v. Lamb, 945 F. Supp. 441, 461-63 (N.D.N.Y. 1996)* (holding that removal and off-site inspection is a reasonable approach for determining whether something is contraband when the determination cannot be made on the spot).

United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), is not to the contrary. Tamura involved a warrant authorizing seizure of three categories of business records. When FBI agents arrived to execute the warrant, they realized it would take a considerable time to separate the materials, so they seized all the company's accounting records [*23] for the period in question, whether covered by the warrant or not. They separated the seizable from the non-seizable materials later at the FBI offices. The Ninth Circuit held that the government's wholesale seizure of company documents was illegal because the agents intentionally seized materials they knew were not covered by the warrant. Here, by contrast, the officers were authorized by the warrant to seize all computer storage media--which is precisely what they did. Significantly, *Tamura* did not hold that a warrant would be too broad if it authorized wholesale seizure of materials that contain both evidence of crime and innocuous matter, if the two kinds of materials are too difficult or time-consuming to separate at the scene. To the contrary, the Tamura court suggested, albeit in dicta, that such a warrant would be appropriate:

> If the need for transporting the documents is known to the officers prior to the search, they may apply for specific authorization for large-scale removal of material, which should be granted by the magistrate issuing the warrant only where on-site sorting is infeasible and no other practical alternative exists.

Id. at 596 [*24] (citing *United States v. Hillyard, 677 F.2d 1336, 1340 (9th Cir. 1982))*.

The warrant here authorized precisely such a seizure of intermingled materials that are difficult and time-consuming to separate on-site. That the officer seeking the warrant did not make a specific showing to this effect is of no consequence: The difficulties of examining and separating electronic media at the scene are well known. It is doubtless with these considerations in mind that the state court judge authorized seizure of all of defendant's storage media, not merely those containing contraband or evidence of crime.

b. Defendant also argues that the warrant was overbroad because it did not define a "search methodology." He claims that the search should have been limited to certain files that are more likely to be associated with child pornography, such as those with a ".jpg" suffix (which usually identifies files containing images) or those containing the word "sex" or other key words.

Defendant's proposed search methodology is unreasonable. "Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent." *United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998).* [*25] Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.

Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled "flour" or "talcum powder." There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it. The ease with which child pornography images can be disguised--whether

by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated--forecloses defendant's proposed search methodology.

3. The government intends to introduce into evidence "over 1,000 images of child pornography and/or child erotica," which it discovered on two 100 megabyte zip diskettes taken from defendant's home. The government's expert discovered the images through a comprehensive forensic computer analysis using "Encase" [*26] forensic software. Defendant wishes to obtain two "mirror image" copies of the computer media analyzed by the government's expert to allow his own expert to conduct a forensic analysis and his counsel to prepare his defense. The government opposes producing these items, offering instead to permit the defense to view the media in an FBI office and to conduct its analysis in the government's lab.

Federal Rule of Criminal Procedure 16(a)(1)(E) provides:

> Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant.

Rule 16 clearly covers the items defendant has requested. They are "data, photographs, [and/or] tangible objects" within the government's possession. Moreover, they are material to the [*27] preparation of the defense, the government intends to use them in its case-in-chief and they were obtained from defendant. *Rule 16(d)(1)*, however, allows the court to regulate discovery: "At any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief."

The government argues that since child pornography is contraband, defense counsel and his expert should be required to examine the images in the controlled environment of the government facility. The cases cited by the government, though,all involve appeals from district court decisions denying a defendant's motion to compel production. They do not hold that a district court would abuse its discretion if it were to order the government to produce copies of the materials. See, e.g., *United States v. Kimbrough, 69 F.3d 723, 730-31 (5th Cir. 1995)* (upholding the district court's denial of defendant's motion to compel production of a copy of a video containing child pornography); *United States v. Horn, 187 F.3d 781, 792 (8th Cir. 1999)* (upholding the district court's refusal to order the government to produce copies of videos alleged, and [*28] later found, to contain child pornography).

The government analogizes the zip disks to narcotics, arguing that their inspection and analysis by defendant's expert should take place in the government's lab under government supervision. This analogy is inapt. Analysis of a narcotics sample is a fairly straightforward, one-time event, while a thorough examination of the thousands of images on the zip disks will take hours, even days, of careful inspection and will require the ability to refer back to the images as the need arises.

The court concludes that defendant will be seriously prejudiced if his expert and counsel do not have copies of the materials. Defense counsel has represented that he will have to conduct an in-depth analysis of the storage media in order to explore whether and when the various images

were viewed, how and when the images were downloaded and other issues relevant to both guilt and sentencing. The court is persuaded that counsel cannot be expected to provide defendant with competent representation unless counsel and his expert have ready access to the materials that will be the heart of the government's case.

The government's proposed alternative--permitting [*29] the defense expert to analyze the media in the government's lab at scheduled times, in the presence of a government agent--is inadequate. The defense expert needs to use his own tools in his own lab. And, he cannot be expected to complete his entire forensic analysis in one visit to the FBI lab. It took defense counsel between two and three hours to quickly scroll through the 2,300 images in the Encase report, so it is likely to take the expert much longer than that to conduct a thorough analysis. Defendant's expert is located in another state, and requiring him to travel repeatedly between his office and the government's lab--and obtain permission each time he does so--is unreasonably burdensome. Moreover, not only does defendant's expert need to view the images, his lawyer also needs repeated access to the evidence in preparing for trial.

There is no indication that defendant's counsel or expert cannot be trusted with the material. The expert is a former government agent who has a safe in his office and has undertaken to abide by any conditions the court places on his possession of the materials. He has experience in dealing with child pornography and takes precautions to ensure [*30] that contamination doesn't occur, including using the Encase software and fully "wiping" the forensic computers on which he examines the images. Defense counsel is a respected member of the bar of this court and that of the Ninth Circuit. The court has every confidence that he can be trusted with access to these materials.

After the court's oral ruling, the parties produced a stipulation setting forth procedures to be employed by defense counsel and his expert in the handling of these materials, and the court has adopted it as its order. Because the court believes that these safeguards provide a useful framework for how such materials can be handled, the relevant portion of the stipulation is reproduced as an appendix to this opinion.

***

The facts alleged in the affidavit were sufficient for the state court judge to conclude that there was probable cause; the warrant she issued was not overbroad. Defendant's motion to suppress is therefore DENIED. Defendant's motion for discovery is GRANTED.

Alex Kozinski

United States Circuit Judge

DATED: June 17, 2004